INTELLIGENCE · MARKET AND COMPETITIVE INTELLIGENCE

The Ethics and Legality of Competitive Intelligence

Competitive intelligence is legitimate and valuable, but it operates close to legal and ethical boundaries. This article explains the laws that govern it, the ethical principles that go beyond the law, why good people cross the line, and how organisations can build practices that keep intelligence work clean.

ModQu research article · 2,579 words · 23 references (APA 7th edition)

Every organisation wants to know what its competitors are doing. Gathering and analysing that information, competitive intelligence, is a normal and valuable part of business. Most of it relies on public sources: annual reports, patents, job advertisements, trade shows, conversations with customers and examination of competitors' products. But the activity sits close to lines that should not be crossed. Posing as a customer to extract pricing details, encouraging a competitor's employee to reveal confidential plans, or searching a rival's rubbish are not merely bad manners. Depending on the circumstances, they may be unlawful, and they are almost always unethical.

This article explains the legal framework that governs competitive intelligence, the ethical principles that apply beyond the law, the psychological and organisational reasons why people cross ethical lines, and the practices that help organisations stay on the right side of them.

Why ethics matters in competitive intelligence

It might seem that competitive intelligence is simply a matter of gathering as much information as possible by whatever means are not explicitly prohibited. Several considerations show why this view is mistaken.

First, the legal risks are serious. Misappropriating trade secrets can lead to large damages, injunctions and, in some jurisdictions, criminal prosecution. Second, the reputational risks are often greater than the legal ones. When unethical intelligence-gathering becomes public, the damage to customer and partner trust can far exceed any value of the information obtained. Third, unethical methods are usually unnecessary. Kahaner (1996) and Fleisher and Bensoussan (2015) both emphasise that the great majority of useful competitive intelligence comes from open and legitimate sources; skilled analysis of public information is more valuable than stolen fragments. Fourth, an organisation that tolerates deception against competitors may find it difficult to sustain honesty internally.

Carroll (1991) described corporate responsibilities as a pyramid: economic responsibilities at the base, then legal responsibilities, then ethical responsibilities to do what is right and fair beyond what the law requires, and finally discretionary or philanthropic responsibilities. Competitive intelligence engages the middle two levels: it must comply with the law and, beyond that, with widely shared standards of fair dealing.

The legal framework

The laws relevant to competitive intelligence vary by country, but several areas are common.

Trade secrets

A **trade secret** is commercially valuable information that is not generally known and that its owner takes reasonable steps to keep secret: a formula, a manufacturing process, customer lists, pricing strategies or plans for new products. Trade secret law protects such information against **misappropriation**, meaning acquisition by improper means, such as theft, bribery, misrepresentation or inducing a breach of confidence, or use and disclosure in breach of a duty.

In the United States, the Economic Espionage Act of 1996 made the theft of trade secrets a federal crime, with heavier penalties where the theft benefits a foreign government. The Defend Trade Secrets Act of 2016 added a federal civil remedy, allowing owners to sue for misappropriation in federal courts. Other countries protect trade secrets through a combination of contract law, equitable duties of confidence and specific statutes.

Importantly, trade secret law does not prohibit learning information through legitimate means. Independent discovery, reverse engineering of a lawfully purchased product, and analysis of public information are generally lawful. The question is how the information was obtained.

Almeling et al. (2010), analysing trade secret cases in American federal courts, found that in the large majority of cases the alleged misappropriator was someone the owner knew, most often an employee or a business partner, not a stranger. The finding underlines the importance of employees' and partners' duties of confidentiality, and of how competitors approach former employees.

Competition law

Competition law, also known as antitrust law, limits what competitors may share with one another. In Canada, the Competition Act (1985) makes it a criminal offence for competitors to agree to fix prices, allocate markets or restrict output, and civil provisions address other agreements that substantially lessen competition. Exchanges of competitively sensitive information, such as current or future prices, between competitors can be evidence of such agreements or can facilitate coordination even without an explicit agreement.

This creates a specific risk for competitive intelligence: gathering information about a rival's prices from public sources is lawful, but obtaining it directly from the rival, or through a shared third party in a way that lets competitors coordinate, can be unlawful. Benchmarking studies and industry surveys should be designed so that individual firms' current sensitive data are not revealed to competitors.

New technologies add new questions. Ezrachi and Stucke (2016) argue that pricing algorithms that monitor and respond to rivals' prices may facilitate tacit collusion. Calvano et al. (2020) showed in simulations that self-learning pricing algorithms could learn to sustain prices above competitive levels without any communication between them. Organisations using automated pricing intelligence should consider these risks.

Privacy law

Competitive intelligence sometimes involves information about individuals: a competitor's executives, sales staff or customers. Privacy laws govern how personal information is collected, used and disclosed. In Canada, the Personal Information Protection and Electronic Documents Act (2000) requires organisations to collect personal information only for purposes a reasonable person would consider appropriate, generally with consent, and to protect it. Acquisti et al. (2015) document how people's expectations of privacy are often violated by data practices they do not see, and Martin et al. (2017) found that firms suffering data privacy failures experienced negative effects on performance, which transparency and customer control could mitigate.

Other laws

Depending on the method, competitive intelligence may also engage laws on computer misuse (accessing systems without authorisation), trespass, fraud and misrepresentation, interception of communications, and breach of contract.

Ethics beyond the law

The law sets a minimum. Many intelligence methods are lawful but still wrong, and many organisations and professional associations set higher standards.

Paine (1991) analysed the ethics of competitor intelligence gathering and identified categories of questionable practices. **Misrepresentation** involves deceiving people about one's identity or purpose: posing as a job candidate, student, journalist or potential customer to obtain information. **Improper influence** involves inducing people to betray obligations, for example by offering jobs or payments to a competitor's employees in exchange for confidential information. **Covert surveillance** involves secretly observing or recording, such as hidden cameras, eavesdropping or searching rubbish. Paine argued that these practices are wrong because they violate principles of honesty, respect for others' obligations and fair competition, regardless of whether a specific law forbids them.

Crane (2005) argued that competitive intelligence becomes industrial espionage when it involves illegal or unethical methods, such as trespass, theft, misrepresentation or breaching confidentiality, or when it harms the public interest. Crane proposed that ethical judgement should consider the tactics used, the nature of the information sought and the purpose for which it will be used.

Principles from research ethics also apply when intelligence is gathered through interviews or surveys. The Belmont Report (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979) set out respect for persons, beneficence and justice as the core principles for research involving people, with informed consent as their practical expression. A competitive intelligence interviewer who conceals the purpose of an interview, or the identity of the client, denies the interviewee the chance to decide what to share.

Calof and Wright (2008) note that professional competitive intelligence associations have developed codes of ethics that commit practitioners to comply with the law, disclose their identity and organisation accurately before interviews, and respect requests for confidentiality.

Hard cases

Some situations are not covered by simple rules and call for judgement. Four recur often.

Hiring from a competitor. Recruiting a competitor's employees is lawful and normal. Their general skills and experience become legitimately available to the new employer. Their former employer's trade secrets and confidential information do not. A new hire who brings documents, customer lists or detailed knowledge of confidential plans exposes the hiring company to legal action. Good practice includes asking new hires to confirm in writing that they have brought no confidential material, instructing them not to use or disclose former employers' secrets, and keeping them away from projects where the risk of misuse is high for a period.

Trade shows. Visiting a competitor's stand, collecting brochures and listening to presentations are acceptable. Wearing a misleading badge, posing as a customer or pressing junior staff with detailed questions they are not authorised to answer are not. The simplest rule is that intelligence staff identify themselves honestly if asked and accept polite refusals.

Customers and suppliers. Customers often share competitors' quotes to negotiate better terms. Receiving such information unsolicited is generally acceptable; asking customers to pass on documents marked confidential, or to breach their own agreements with suppliers, is not. Similar care applies to shared suppliers who may hold confidential information about several clients.

Information that arrives by accident. Sometimes confidential information arrives unexpectedly: a misdirected email, a document left behind after a meeting, a file accidentally made public. Ethical practice, and in many cases legal prudence, is to stop reading, avoid copying or circulating the material, inform legal counsel and, where appropriate, notify the owner. Using such information can turn an accident into misappropriation.

Differences between countries

Laws and norms differ between jurisdictions. Some countries criminalise trade secret theft; others treat it mainly as a civil matter. Privacy rules are stricter in some regions than others, and the boundaries of acceptable information exchange under competition law vary. Business customs also differ in what is considered acceptable to ask or offer. Organisations operating internationally should apply a consistent standard based on the strictest relevant rules and on their own ethical principles, rather than adopting whatever local practice permits. A method that is legal in one country but would be illegal or scandalous in the organisation's home market creates risks wherever it is used.

Four tests for any collection method

A practical way to apply these principles is to subject every proposed method to four questions, as shown in Figure 1.

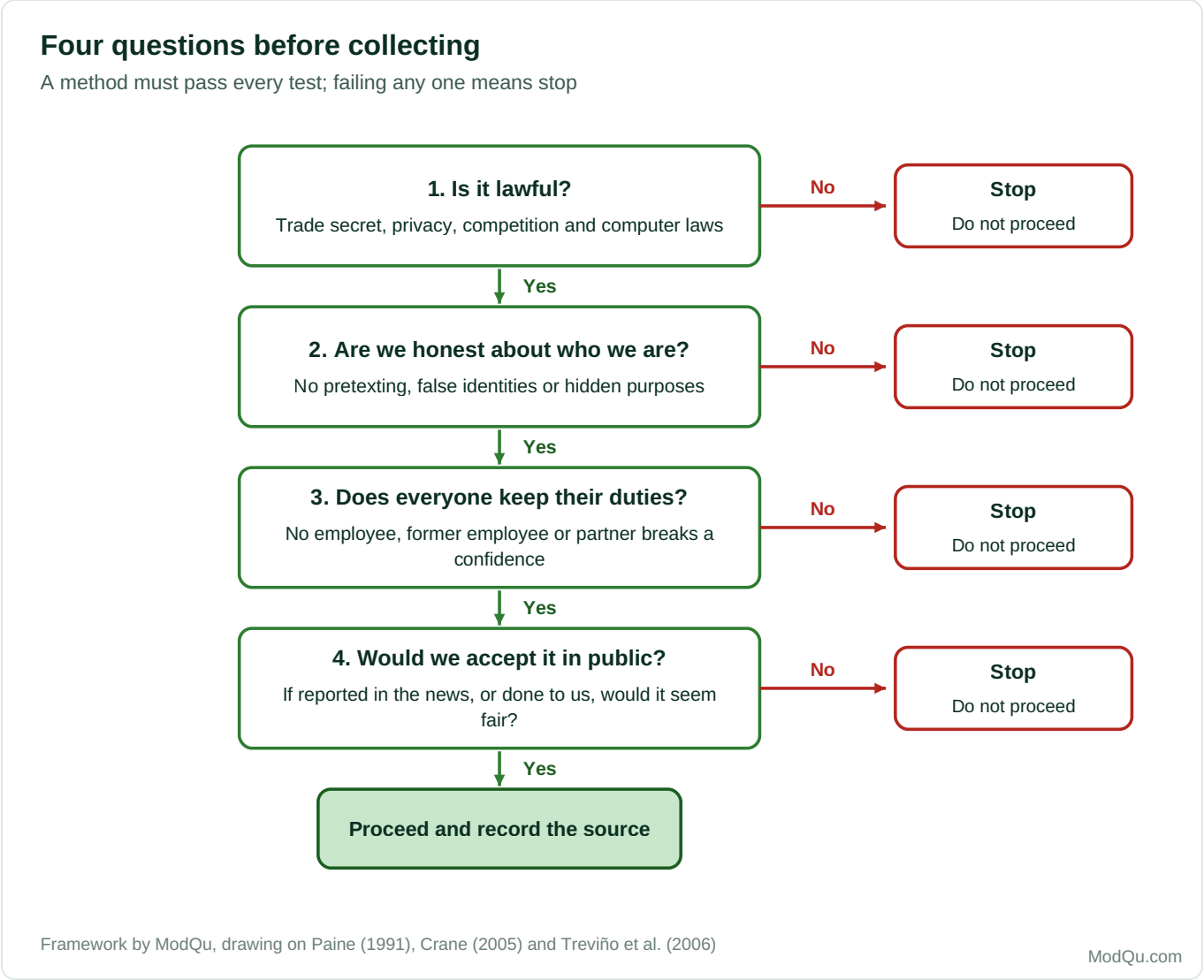


Figure 1. Four questions before collecting. Any method that fails one test should not be used. Framework by ModQu, drawing on Paine (1991), Crane (2005) and Treviño et al. (2006).

The fourth question, sometimes called the newspaper test, captures a useful intuition: methods that would embarrass the organisation if reported publicly, or that it would consider unfair if a competitor used them against it, are likely to be wrong.

Why good people cross the line

Most ethical failures in competitive intelligence are not committed by villains. They are committed by ordinary employees under pressure. Research in behavioural ethics helps explain why.

Treviño et al. (2006), reviewing research on ethical behaviour in organisations, found that unethical conduct results from a combination of individual factors, such as moral awareness and reasoning, and situational factors, such as organisational culture, leadership, rewards and pressure. People are strongly influenced by what their organisations reward and tolerate.

Ethical fading. Tenbrunsel and Messick (2004) describe how the ethical dimensions of a decision can fade from view, especially when decisions are framed in business terms. Calling deception "gathering market data" or "pretexting" makes it seem like a technical choice rather than a moral one.

Moral disengagement. Bandura (1999) identified mechanisms by which people disengage their moral standards: euphemistic labelling, comparing one's conduct with worse behaviour, displacing responsibility to superiors, diffusing it across a group and minimising the harm caused. In intelligence work, statements such as "everyone does it", "the client asked for it" or "it's only a small detail" are typical forms of disengagement.

Goals and incentives. Ordóñez et al. (2009) showed that specific, challenging goals can encourage unethical behaviour, especially when people are close to a target. Kerr (1975) showed how organisations often reward behaviour they do not want. An intelligence team rewarded for "getting the competitor's pricing" without regard to method faces exactly this pressure.

Outsourcing. Organisations sometimes hire external firms to gather intelligence and do not ask how it is obtained. Responsibility does not disappear with outsourcing. A widely reported example occurred in 2001, when Procter & Gamble disclosed that contractors gathering information about Unilever's hair care business had searched rubbish bins outside a Unilever office. Procter & Gamble informed Unilever, returned the documents and reached a settlement, but the episode became a standard example of intelligence gathering gone wrong.

An illustration

A software company's sales director wants to know the discount structure a rival offers to large customers. A junior analyst suggests calling the rival's sales team while posing as a procurement manager at a prospective client. The analyst's manager applies the four tests. The method may not breach a specific law, but it fails the second test, because it misrepresents the caller's identity, and the fourth, because the company would consider it unfair if a rival did the same to it. The manager rejects it.

Instead, the team gathers information openly. It reviews public procurement records, where government contracts often disclose prices; asks its own salespeople to record competitor pricing that prospective customers volunteer during negotiations; and commissions an independent survey of buyers, conducted by a research firm that identifies itself and keeps individual responses confidential. Within two months the company has a reliable picture of the rival's typical discounts by deal size, obtained without deception and documented source by source.

Protecting your own information

Ethics in competitive intelligence has a defensive side. Organisations should assume that competitors are studying them and protect their own sensitive information. Hannah (2005) found that employees were more likely to see themselves as obliged to protect trade secrets when their employers used clear protection procedures, such as marking documents as confidential and explaining why information mattered. Training staff to recognise improper approaches, such as unusually probing questions from unknown callers or "students", reduces leakage.

Building an ethical intelligence practice

Several practices help organisations gather intelligence effectively and ethically:

1. **A written policy.** Set out permitted, restricted and prohibited methods, with examples, and require approval for anything in the restricted category.
2. **Training.** Teach everyone involved in intelligence work, including salespeople who gather information informally, how to apply the policy.
3. **Honest identification.** Require interviewers to state their name and organisation, and to respect refusals.
4. **Respect for confidentiality.** Never ask current or former employees of competitors to disclose confidential information, and stop conversations that move in that direction.
5. **Control of contractors.** Include the policy in contracts with external intelligence providers, ask how information was obtained and audit their methods.
6. **Source records.** Record the source of each important piece of information so that its legitimacy can be shown if questioned.
7. **Legal review.** Involve legal counsel in benchmarking, industry data-sharing and any method near a legal boundary.
8. **Leadership and incentives.** Reward good analysis rather than the acquisition of secret information, and make clear that no business objective justifies improper methods.

Gilad (2004) argues that the real value of competitive intelligence lies in early warning and insight, not in secrets. Organisations that internalise this view have little reason to cross ethical lines, because their advantage comes from thinking better about information available to all.

Conclusion

Competitive intelligence is a legitimate and valuable activity, but it operates near legal and ethical boundaries. Trade secret, competition, privacy and other laws set minimum standards; ethical principles of honesty, respect for others' obligations and fair competition set higher ones. Research shows that people cross these lines mainly under organisational pressure, through euphemism and disengagement rather than deliberate wrongdoing. Clear policies, training, honest practices, control of contractors and leadership that values analysis over secrets allow organisations to gather intelligence that is both useful and clean.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Almeling, D. S., Snyder, D. W., Sapoznikow, M., McCollum, W. E., & Weader, J. (2010). A statistical analysis of trade secret litigation in federal courts. *Gonzaga Law Review, 45*(2), 291–334.

Bandura, A. (1999). Moral disengagement in the perpetration of inhumanities. *Personality and Social Psychology Review, 3*(3), 193–209. https://doi.org/10.1207/s15327957pspr0303_3

Calof, J. L., & Wright, S. (2008). Competitive intelligence: A practitioner, academic and inter-disciplinary perspective. *European Journal of Marketing, 42*(7/8), 717–730. https://doi.org/10.1108/03090560810877114

Calvano, E., Calzolari, G., Denicolò, V., & Pastorello, S. (2020). Artificial intelligence, algorithmic pricing, and collusion. *American Economic Review, 110*(10), 3267–3297. https://doi.org/10.1257/aer.20190623

Carroll, A. B. (1991). The pyramid of corporate social responsibility: Toward the moral management of organizational stakeholders. *Business Horizons, 34*(4), 39–48. https://doi.org/10.1016/0007-6813(91)90005-G

Competition Act, R.S.C. 1985, c. C-34 (Canada).

Crane, A. (2005). In the company of spies: When competitive intelligence gathering becomes industrial espionage. *Business Horizons, 48*(3), 233–240. https://doi.org/10.1016/j.bushor.2004.11.005

Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (2016).

Economic Espionage Act of 1996, 18 U.S.C. §§ 1831–1839 (1996).

Ezrachi, A., & Stucke, M. E. (2016). *Virtual competition: The promise and perils of the algorithm-driven economy*. Harvard University Press.

Fleisher, C. S., & Bensoussan, B. E. (2015). *Business and competitive analysis: Effective application of new and classic methods* (2nd ed.). Pearson Education.

Gilad, B. (2004). *Early warning: Using competitive intelligence to anticipate market shifts, control risk, and create powerful strategies*. AMACOM.

Hannah, D. R. (2005). Should I keep a secret? The effects of trade secret protection procedures on employees' obligations to protect trade secrets. *Organization Science, 16*(1), 71–84. https://doi.org/10.1287/orsc.1040.0113

Kahaner, L. (1996). *Competitive intelligence: How to gather, analyze, and use information to move your business to the top*. Simon & Schuster.

Kerr, S. (1975). On the folly of rewarding A, while hoping for B. *Academy of Management Journal, 18*(4), 769–783. https://doi.org/10.5465/255378

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing, 81*(1), 36–58. https://doi.org/10.1509/jm.15.0497

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). *The Belmont report: Ethical principles and guidelines for the protection of human subjects of research*. U.S. Department of Health, Education, and Welfare.

Ordóñez, L. D., Schweitzer, M. E., Galinsky, A. D., & Bazerman, M. H. (2009). Goals gone wild: The systematic side effects of overprescribing goal setting. *Academy of Management Perspectives*, *23*(1), 6–16. https://doi.org/10.5465/amp.2009.37007999

Paine, L. S. (1991). Corporate policy and the ethics of competitor intelligence gathering. *Journal of Business Ethics*, *10*(6), 423–436. https://doi.org/10.1007/BF00382825

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (Canada).

Tenbrunsel, A. E., & Messick, D. M. (2004). Ethical fading: The role of self-deception in unethical behavior. *Social Justice Research*, *17*(2), 223–236. https://doi.org/10.1023/B:SORE.0000027411.35832.53

Treviño, L. K., Weaver, G. R., & Reynolds, S. J. (2006). Behavioral ethics in organizations: A review. *Journal of Management*, *32*(6), 951–990. https://doi.org/10.1177/0149206306294258